Testimony of
Joseph M. Weiss
Control Systems Cyber Security Expert

before the

Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
U.S. House of Representatives

October 17, 2007

Control Systems Cyber Security—The Need for Appropriate Regulations to Assure the Cyber Security of the Electric Grid

Joseph M. Weiss, PE, CISM
Managing Partner, Applied Control Solutions, LLC

Good afternoon Mr. Chairman and Members of the Committee. I would like to thank the Committee for your invitation to discuss the need for appropriate cyber security of the control systems utilized in our nation's critical infrastructure, in particular, the electric infrastructure.

I am a nuclear engineer who has spent more than thirty years working in the commercial power industry designing, developing, implementing, and analyzing industrial instrumentation and control systems. I have performed cyber security vulnerability assessments of power plants, substations, electric utility control centers, and water systems. I am a member of many groups working to improve the reliability and availability of critical infrastructures and their control systems, including the North American Electric Reliability Council's (NERC) Control Systems Security Working Group (CSSWG), the Instrumentation Systems and Automation Society (ISA) S99 Manufacturing and Control Systems Security Committee, the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF), Institute for Electrical and Electronic Engineers (IEEE) Power Engineering Society Substations Committee, International ElectroTechnical Commission (IEC) Technical Committee 57 Working Group 15, and Council on Large Electric Systems (CIGRÉ) Joint Working Group D2.22. As a control system cyber security expert, citizen, stockholder, and ratepayer, I am very concerned about the electric industry's approach to securing the electric grid. I would like to state for the record that the views expressed in this testimony are mine. I am not representing any of the groups in which I am involved.

Until 2000, my focus strictly was to design and develop control systems that were efficient, flexible, cost-effective, and remotely accessible, without concern for cyber security. At about that time, the idea of interconnecting control systems with other networked computing systems started to gain a foothold as a means to help lower costs and improve efficiency, by making available operations-related data for management "decision support." Systems of all kinds that were not interconnected with others and thereby could not share information ("islands of automation") became viewed as an outmoded philosophy. But at the same time, there was no corresponding appreciation for the cyber security risks created. To a considerable extent, a lack of appreciation for the potential security pitfalls of highly interconnected systems is still prevalent today, as can be witnessed in a recent article in the September 2007 issue of Power Magazine[1]. As such, the need for organizations to obtain information from

[1]Makansi, Jason, "Integrated Software Platform Eludes Many Owner/Operators", Power Magazine, September 2007.

operational control system networks to enable ancillary business objectives has often unknowingly led to increased cyber vulnerability of control system assets themselves.

Generally cyber security has been the purview of the Information Technology (IT) department, while electric control system departments have focused on grid and plant operations efficiency and reliability – not cyber security. This has led to the current situation where some parts of the organization are now sensitized to security while others are not as yet aware of the need. Industry has made progress in identifying control system cyber security as an issue while not appreciating the full gravity of the matter. In other ways, particularly concerning the proposed NERC Critical Infrastructure Protection (CIP) cyber security standards[2], I believe we have fallen short of the mark. The timing of this hearing is fortuitous as more than 70 organizations have recently submitted commentary responses to the Federal Energy Regulatory Commission's (FERC) Notice of Proposed Rulemaking (NOPR) RM06-22[3]. These submittals provide a detailed view into the electric power industry's intended approach to securing the cyber assets used to operate the grid.

How Mainstream IT and Control System Cyber Security are Different

Control systems include distributed control systems (DCS), programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, and related networked-computing systems. Control systems are designed and operated differently than mainstream IT business systems. Traditionally, the emphasis in securing business IT systems is to employ the best practices associated with the well-established "Confidentiality, Integrity, Availability" (CIA) triad model – in that order of importance. Typically extra emphasis is placed on rigorous human end user access control and data encryption to satisfy the important function of confidentiality. In control systems, however, confidentiality has less urgency than system availability and data integrity, because in actual control system operation, the typical "users" are other computer-based devises (e.g. PLCs and field devices), not humans. This distinction, and the fact that most extant control systems are outfitted with older microprocessors with little compute power, lies at the heart of the issue of securing control systems in a manner appropriate to current need.

Unfortunately, today very few people possess thorough understanding of control system cyber security. This understanding requires prior detailed knowledge of the control system application, how it is designed and operated, as well as how it communicates and is interconnected with other systems and ancillary computing assets, before appreciation of cyber vulnerabilities of the system as a whole can begin. Figure 1 generally characterizes the relationship of the different types of specialty technical skills needed for control system cyber security expertise, and also reflects the relative quantities of each at work in industry today. Most people now becoming involved with control system cyber security typically come from a mainstream IT background and not that of control systems. This has, in some cases, inadvertently resulted in making control systems less reliable without providing increased security, such as the example of the uninformed use of mainstream IT port scanners on older generation PLC networks.

[2] NERC Cyber Security Standards, http://www.nerc.com/~filez/StandardsStandards/Cyber-Security-Permanent.html
[3] Federal Energy Regulatory Commission Docket RM06-22, http://www.ferc.gov/docs-filing/elibrary.asp

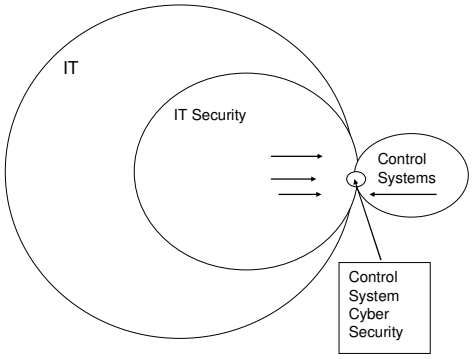

Figure 1 - Relationship and Relative Availability of Control System Cyber Security Expertise

It is often mistakenly assumed that a cyber security incident is always a premeditated targeted attack. However, NIST defines a Cyber Incident[4] as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability (CIA) of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. Incidents may be intentional or unintentional." Unintentional compromises of CIA are significantly more prevalent and can have severe consequences. In fact, statistics collected over roughly the past 20 years in mainstream IT have consistently shown that about two-thirds of all cyber security incidents originate from within an organization, and that the cause of most of those are unintentional human error. This phenomenon must also be addressed by cyber security standards if they are to be effective.

Use of mainstream operating system environments such as Windows and UNIX for running control system applications leave them just as vulnerable as these operating systems are when used anywhere else, and application of mainstream IT security technical solutions and/or methods can be applied to help secure our more modern control system host computers and operator consoles (i.e., PCs). At the same time, however, application of mainstream IT security technologies and methods can also adversely affect the operation of control systems, such as causing components on networks of older generation PLCs to freeze-up upon use of port scanning tools, as noted. Furthermore, DOE's Idaho National Laboratory (INL) has conducted demonstrations of how a hacker can manipulate widely used "middleware" software running on very current mainstream computer systems without a great deal of difficulty, e.g., using vulnerabilities in OPC code ("OLE for Process Control"). In this sobering demonstration the system appears to be functioning properly even though it is not; while displaying incorrect information to, or withholding correct information from, system operator consoles.

Inadequacy of NERC CIP Standards as Effective Regulation

Prior to NERC becoming the Electric Reliability Organization (ERO), NERC was an industry sponsored, industry-led, and industry-funded organization, and they still are today. Contrary to popular belief, NERC as ERO is still funded by the industry, thereby creating potential for conflict of interest. It was a secret to no one involved that the objective in drafting the Critical Infrastructure Protection (CIP) Standards was

[4] National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

for the industry, through NERC, to put something in place to its liking before the Federal Government did so in its behalf. Thus, the CIP Standards were developed by a trade association.

Because NERC employs an American National Standards Institute (ANSI)-approved standards development process, it is required to follow certain rules including balloting of its standards to obtain approval from constituent industry member organizations. Consequently, as the CIP Standards went through the balloting process, they became less inclusive, more ambiguous, and created more exemptions to applicability. It should also be noted that prior to industry acceptance of the final version, the CIP Standards went though three rounds of drafting and subsequent industry comment of approximately 1000 pages each (with some redundancy), and the NERC Drafting Team could accept or reject recommendations unilaterally as they deemed appropriate, with but modest explanation as to rationale. NERC and many utility representatives recognized the limitations of this effort, but felt anything more rigorous in terms of requirements would not be acceptable to enough utility organizations to pass ballot.

As the NERC CIP Standards moved to their final revision, the focus was shifted entirely to bulk power grid reliability in and of itself, rather than on societal welfare and safety from a homeland security or economic perspective. The reliable operation of a small substation that supports a major oil or gas pipeline in a remote locale is not salient to grid stability, but failure of same could very well have profound adverse consequences for the health of the US economy. Likewise, under the CIP Standards, the importance of continuity of electric power to municipal water works, manufacturing plants, refineries, hospitals, and military installations, etc., is not a factor requiring consideration in determining the importance (or "Criticality") of the electric system assets which serve them.

Perhaps the biggest issue with the CIP Standards as a set is CIP-002, which establishes the scope of applicability for all of the other CIP Standards: identification of "Critical Assets." These are individual pieces of electric system equipment such as electric generating units, substation transformers and digital protective relays, and though not explicitly stated, presumably though not explicitly the control system hosts, related servers, and operator consoles as well. Per CIP-002, deciding exactly which electric system assets are critical to reliable operation of the bulk electric system is left up to each individual organization to determine for itself, using a "risk based assessment methodology" of its own choosing or design. It is only the network-computing control systems components used to operate these specific Critical Assets – thereby deemed "Critical Cyber Assets" – that must be protected under the CIP Standards. For all other non-Critical electric and control system assets, the CIP Standards simply do not apply and may be ignored. As CIP-002 is currently written, allowing an organization to choose its own methodology permits the documented results from the flip of the coin as a perfectly valid and compliant approach to self-determination of Critical Assets. FERC has expressed consternation with this "flexibility" in its Notice of Public Rulemaking (NOPR) comments, and in its Final Rule will in all likelihood remand this Standard back to the NERC Standards process for re-conception. Unfortunately, the NERC standards development process takes a great deal of time, and our enemies are not constrained to only take advantage of our vulnerabilities after our schedule for securing them has run its course. The industry has been in the process of developing cyber security standards for over four years, and yet the matter remains unconcluded.

As noted, the CIP Standards apply only to those electric system components self-identified by asset owners themselves to be critical to their ability to maintain reliability for that part of the bulk electric grid falling under the aegis of each. The process does not embrace intra-region, inter-region, or a national viewpoint of the grid as a system, but rather only parochial considerations, each in isolation to the others. Additionally, there is no requirement to take into consideration the potential for multiple contingency threat scenarios that can involve more than one sphere of interest, such as interdependency of critical natural gas pumping stations and the greater electric power system. What's more, because utilities are

interconnected, they often share equipment where the utilities conjoin (e.g., "dual ported Remote Terminal Units-RTUs"), to say nothing about network-to-network data router interconnections. Accordingly, because utilities will apply the CIP Standards in a non-uniform fashion, one utility's less rigorous application of the CIP requirements will make it a "weak link" relative to its neighbor utility, to the detriment of the cyber security of both organizations and any others to which there are further data network interconnections. Also note that all major electric sector control systems in North America communicate over the common "NERCnet", further exacerbating the situation. Worse yet, these days most control networks are also interconnected with their corporate IT networks, which themselves are connected to the Internet. A chain is only as strong as its weakest link.

Technically, the CIP Standards were conceived primarily from the frame of reference of protecting control center host systems and operator consoles, rather than field and plant floor controls equipment ("Other Facilities") at work in substations, switchyards, and power plants. The data systems in use within control centers generally utilize current computing and networking technology, requiring protective measures akin to those used in mainstream business and Internet computing. Conversely, most field PCS (e.g., substation equipment) and power plant DCS controller equipment still in use today employ technology that generally is obsolete and has little in the way of built-in cyber defenses, with little potential for upgrade or augmentation. But since the CIP Standards are intended to apply for both data center and intelligent field assets, they had to be written in a way that would be relevant for advanced current and future computing technologies, while at the same time accommodating what is essentially 'ancient' field and plant controls equipment. The result is milquetoast one-size fits all standards that are not rigorous enough for current and future cyber security challenges on the one hand, and by and large are overkill for the older field and plant cyber assets still in use. What's more, major gaps in CIP Standards' effectiveness are created by a number of explicit exclusions from applicability – in essence, loopholes.

Ironically, some of the most important contributors to grid reliability, nuclear power plants, are excluded from the scope of consideration as to criticality. While the Nuclear Regulatory Commission (NRC) has robust physical security standards for nuclear plants, the interconnection of nuclear power plant cyber control assets with those used to manage the bulk electric grid currently is *not* addressed in *either* NERC or NRC Standards. Also, while physical security requirements are specified by NRC for nuclear power plants, a little appreciated subtlety is that the CIP Standards specify physical security requirements for Critical *Cyber* Assets *only*. There is no existing NERC standard governing physical security of the Critical Assets themselves, or any other grid assets for that matter.

Since electric distribution systems have been excluded from CIP Standards' scope, so too are the controls used to operate them. This is true even though distribution assets are in operation within many transmission substations. Regardless of this, while many distribution systems employ no control system at all, the ones that do are electronically interconnected with transmission control systems, thereby creating a direct pathway into the networked-controls infrastructure of the greater bulk electric grid. Independent System Operator (ISO) and Regional Transmission Operator (RTO) energy management systems (EMS) are intrinsically data networks, interconnected one with another via NERCnet. Also via NERCnet, each is also interconnected with "downstream" control systems operated by more localized distribution operators, including cooperatives and municipal utilities. With control systems of all ownership becoming increasingly interconnected to one another, while also being interconnected with general-purpose corporate data networks and the Internet, control system exposure to cyber threats is greatly increased. Accordingly, the frame of reference concerning standards for control system cyber security supporting grid reliability purposes must be expanded to account for at least those operational control systems that need to be directly interconnected. This means expanding the scope of the standards to include smaller control area systems which routinely exchange data – and potentially viruses, worms, or other possibly compromised data – with ISO/RTO systems directly. Smaller control area systems can be attractive points of entry and through-navigation paths employed in common hacker "island hopping" technique. By

analogy, at least some of the 9/11 terrorists entered the air transit system through feeder airports on that fateful day.

Another exception to applicability of the CIP Standards are control systems' data communication infrastructure per se. Currently, the electric industry has a huge investment in serial communications that will not be replaced and/or upgraded to routable communications such as Internet Protocol (IP) for many years. These serial communication systems have been demonstrated by the National Laboratories to be cyber vulnerable, e.g., through induction coil passive wiretapping or war dialing, and there have been instances where serial communications have been compromised. However, legacy protocol serial communications are excluded from the CIP Standards' scope simply because they employ non-routable protocols.

A further dubious exclusion from the scope of CIP Standards' applicability involves the Open Access Same-Time Information System (OASIS). These distributed market trading systems are excluded from CIP scope, even though they are routinely connected to energy management systems (EMS) and/or SCADA reliability systems on one side, and the Internet on the other. There is no existing regulation currently governing the cyber security of market systems, which many large systems operators will tell, at least privately, are paramount to their ability to dispatch their reliability responsibilities. In fact, aside from OASIS systems becoming entirely unavailable, an operations manager for a large transmission organization recently offered in confidence that "the thing that scares [him] most in terms of maintaining reliability is spoofed [OASIS] schedules and tags" through cyber means.

Finally, while some electric industry organizations are using ambiguities within the CIP Standards to minimize the number of Critical Cyber Assets to which the Standards must be applied, without realizing it they may be greatly increasing their liability in other ways. At the ISA Expo2007 in Houston[5], a panel session was held on October 2, 2007, covering NERC CIP implementation. The NERC representative in attendance explicitly stated that a utility would be CIP-compliant merely by establishing cyber security policies of some kind, even if they are poorly conceived or effectively inadequate to need. During the CIP Standards drafting process a less vocal but substantial number of electric industry representatives complained about the absence of "adequacy metrics" pertaining to the Standards' requirements in general across the board, which was not remedied prior to their balloted approval by the industry. This demonstrates how conception of the CIP Standards has missed the mark of thoughtfully effecting genuine cyber security, but rather has resulted in the framing of a compliance exercise in essence amounting to adherence to a checklist. This at once elevates the need for technically competent auditors who can review the checklists and ask the right questions, while at the same time there are very few auditors who have requisite experience in the context of control systems. What's more, during a panel session at the ISA Expo2005 in Chicago, one utility industry representative presented the following slide: "In the Electric Sector, the Business Case for CIP & Reliability initiatives in today's landscape must be based on the surety that your company will be financially impacted if it is found to be noncompliant."[6] That is, if the amount of the fine would be less than the cost to become secure, the utility would pay the fine.

Case Histories Which Reveal NERC CIP Standards' Inadequacies

Contacts throughout industry have shared with me the details and adverse affects of more than 90 confirmed control system cyber security incidents to date. This information has been shared with me by individuals from the affected organizations, and from government sources such as the Nuclear Regulatory Commission (NRC), the DOE National Laboratories, the National Transportation Safety Board (NTSB), and the National Institute of Standards and Technology (NIST). Note use of the term "incident", not

[5] Panel Session on NERC Compliance, ISAExpo2007, Houston, TX, October 2, 2007.
[6] Thomas Flowers, "The Business Case for Being Auditably Compliant", ISAExpo2005, Chicago, IL, October 25, 2005.

"attack", as most of these events have been unintentional. The incidents are international in scope (North America, Europe, and Asia) and span several industrial infrastructures including electric power, water, oil/gas, chemical, and manufacturing. With respect to the electric power industry, cyber incidents have occurred in transmission, distribution, and generation including fossil, hydro, and nuclear power plants. Impacts, whether intentional or unintentional, range from trivial to significant environmental discharges, serious equipment damage, and even death. Figure 2 shows the result of a Bellingham, WA, pipe rupture[7], which an investigation concluded was not caused by an intentional act. Figure 3 is a picture from the Idaho National Laboratory (INL) demonstration of the ability to intentionally destroy an electric generator by simulating a cyber attack.[8]

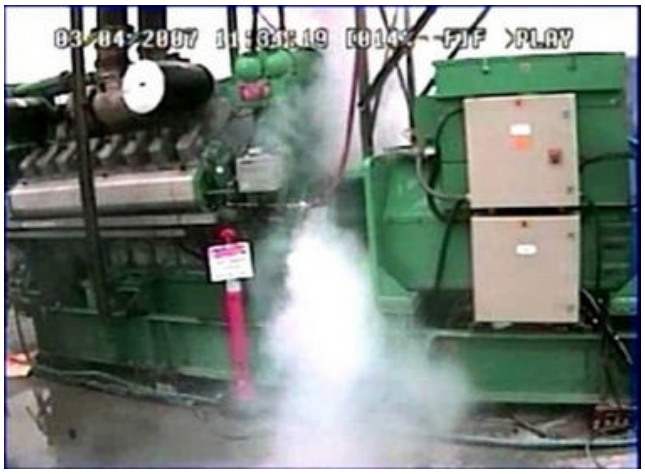

Figure 2 Bellingham, WA Gasoline Pipeline Rupture Figure 3 INL Cyber Demonstration

The deficiencies in the NERC CIP can be demonstrated by the exercise of applying them to historical cyber events. In each historical case discussed below, adherence to CIP Standards' requirements would have failed to address the underlying causes. I have chosen events that are all publicly documented by government (US and Australian) reports. I have also included references to the Final Report of the 2003 Northeast Blackout[9]. The reason for including this reference example is because there were several cyber issues associated with the Northeast Blackout including co-temporal release of the Blaster worm and the First Energy SCADA system alarm problem. These issues resulted in 13 (of the 46) recommendations contained in the Northeast Blackout Report being cyber-related. The Northeast Outage Final Report was issued approximately two years before the NERC CIP Standards were approved. Not including the Blackout Report's recommendations is inexcusable.

Case 1) June 20, 2003 "SQL Slammer Worm Lessons Learned…"[10].

The control network at issued employed a frame relay data network service that interfaces with both the utility's host control system on one side of the network, and field components on the other. This network service, vended by a large telecommunications carrier, supported many diverse business organizations

[7] "Pipeline Accident Report Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999", National Transmission Safety Board Report NTSB/PAR-02/02 PB2002-916502.
[8] http://news.yahoo.com/s/ap/20070927/ap_on_go_ca_st_pe/hacking_the_grid_13
[9] Final Report of the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, https://reports.energy.gov/BlackoutFinal-Web.pdf
[10] SQL Slammer Worm Lessons Learned for Consideration by the Electric Sector, June 20, 2003, nerc.com.

simultaneously. As is common, this network service utilized a high speed Asynchronous Transfer Mode (ATM) core network backbone at the center of the frame relay network. With the release and rapid spread of the Slammer worm across businesses of all kinds serviced by the frame network, the core ATM infrastructure became choked by the worm's multiplying replication and propagation. This resulted in blockage of SCADA traffic between the utility controls host and remote controls equipment in field substations. Note that NERCnet is a shared frame relay network.

Issues: The telecom network was in essence shut down by Slammer worm traffic. The Final Report on the Northeast Blackout recommends the development of a capability to detect wireless and remote wire line intrusion and surveillance, and this report was issued prior to the adoption of the NERC CIP Standards. NERC should have heeded this recommendation, but inexplicably, the CIP Standards exclude availability requirements for telecom networking, which is intrinsic to control system operations. As will be discussed later, the NIST SP800-53 standard does not allow a scope exclusion concerning telecommunications network availability – the CIP Standards do.

Case 2) Tempe, Arizona Area Outage of June 29, 2007 [11].

The outage lasted 46 minutes and affected 98,700 customers, representing 399 Megawatts (MW) of load. It was caused by the unexplained activation of the distribution load shedding program in the energy management system (EMS) at the Salt River Project (SRP), the utility affected. A total of 141 distribution circuit breakers were opened by the EMS unexpectedly.

Issues: Most of the automation used in electric transmission and distribution systems is used to manage the distribution function. Distribution systems can be directly connected to transmission systems, and distribution system failures can be precursors to cascading outages resulting from runaway load shedding. However, the NERC CIP excludes distribution automation from scope, because they are not deemed to be part of the bulk electric system per se (i.e., the grid). NIST SP800-53 does not allow exclusion from scope of distribution automation assets.

Case 3) Australian Wireless Network Hack[12]

A disgruntled former consultant to an Australian firm that used radio-controlled SCADA sewage processing equipment packed his car with stolen radio equipment and attached it to a computer. He drove around the area on at least 46 occasions from February 28 to April 23, 2000, issuing radio commands to open discharge valves, resulting in sewage spills. This attack became the first widely known example of someone maliciously breaking into a control system.

Issues: Aware of this event, the task force that issued The Final Report of the Northeast Blackout recommended the development of capabilities to detect wireless and remote wire line intrusion and surveillance. The Blackout Report and the Australian sewage attack report were issued prior to the issuance of the NERC CIPs. Inexplicably, the NERC CIP Standards exclude non-routable protocols and do not explicitly address wireless communications. NIST SP800-53 does not have these scope exclusions concerning non-routable protocols, and addresses wireless communications explicitly.

[11] "Computer Problem Causes Brief Outage to as Many as 100,000 SRP Customers in Arizona", Energy Assurance Daily, Friday June 29, 2007, http://www.oe.netl.doe.gov/docs/eads/ead062907.pdf

[12] Supreme Court of Queensland r v Boden, Vitek 2002, CA Number 324 of 2001 DC Number 340 of 2001, http://www.courts.qld.gov.au/qjudgment/QCA%202002/QCA02-164.pdf.

Case 4) Nuclear Power Plant Cyber Incident[13]

On August 19, 2006, operators at Browns Ferry nuclear generating facility, had to manually scram (shut down) Unit 3 following a loss of both primary and secondary reactor water recirculation pumps. Plant procedures specified that the manual scram was required following the loss of recirculation flow. The NRC issued an Information Notice (IN) to alert licensees about recent operating experience related to the effects of potential interactions and unanticipated failures of Ethernet connected non-safety equipment on the safety and performance systems in use at nuclear power stations.

Issues: Nuclear plants represent approximately 20% of US electric power generation. Widespread shutdown of nuclear facilities would have significant adverse impact on the reliability of the bulk electric grid. The NRC is responsible for the safety of nuclear plants, that is, safe shutdown. NRC does not however "regulate" the continued operation of nuclear plants in relation to grid reliability, as witnessed in the NRC Information Notice. The NERC CIP Standards exclude nuclear power facilities from scope, while NIST SP800-53 does not allow such exclusions for nuclear plants.

Early Repercussions from Establishment of the CIP Standards

As noted above, each organization in the electric industry with responsibility for maintaining the reliability of the bulk electric system is free to adopt a risk based assessment methodology of its own choosing or design to determine which cyber controls apparatus must be protected. Discussion across the industry has born witness to an interesting phenomenon which has yet to be formally documented anywhere. It so happens that many of the largest electric utilities have determined in their risk assessments that they have no – zero – critical generation assets. In fact, within one of the largest regions in the US, the southeast, virtually none of the large operators have identified any of their generation assets – nuclear included – as being critical to reliability of the bulk electric system. The reason for this is offered forthrightly, that their systems have been designed to withstand "N-1 contingencies," meaning that they can withstand the loss of any single unit without adverse impact on reliability. What is not being considered is the potential for simultaneous multiple contingencies. With the greater controls infrastructure being as cyber-interconnected as observed earlier, it is by no means beyond the realm of possibility of just such an occurrence taking place. Without digression into potential permutations, while Slammer and Blaster worms were propagated via email, and email is generally not used in operational control systems, an analogous threat vector could be sculpted for widespread attack on the greater assemblage of control systems used to operate the grid. What if a Trojan Horse planted in numerous generation control systems should awaken at the appointed hour and simultaneously trip a whole collection of plants in a region offline at once? The effect would look very much like the Northeast Blackout. Very possible scenarios such as this are being discounted out of hand by people in positions of authority who really do not understand cyber security.

Second, we are also witnessing an unfortunate and unexpected phenomenon concerning the CIP Standards that leaves us at cross purposes with other needed electric system management improvements. Many of the more recent utility controls automation upgrades have been motivated by the goal of improving electric system reliability, but at the same time to also aid reduction in operation and maintenance costs. Many of these new systems enhancements are predicated upon the use of modern digital networking technologies (e.g., employing routable protocols such as IP), and in so doing these assets explicitly fall within scope of NERC CIP Standards' compliance. Consequently, because of concerns about potentially being "caught by the CIP Standards" in a state of noncompliance thereby resulting in potentially large fines, a number of utilities have started to disconnect, or have ceased implementation of, these modern networked-systems improvements – motivated explicitly by the goal of

[13] NRC Information Notice: 2007-15: Effects of Ethernet-Based, Non Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations, April 17, 2007.

CIP Standards compliance-requirements avoidance. This tactic results in leaving certain existing cyber vulnerabilities unaddressed through exploitation of loopholes in the CIP Standards, as now written. At the same time, new "time and distance compression" operating efficiencies that can be garnered through use of modern networked remote control and telemetry are thereby lost by this step backward. The potential for improved operational efficiency could at least temporarily contain if not indeed reduce gross operating costs, which in turn holds the line on electric rates experienced by society. So, it appears that the industry is at cross-purposes in its response to the need to both secure and modernize the existing control systems infrastructure. This ironic industry response to the CIP Standards serves neither purpose in any discernable positive way.

An Alternative to the NERC CIP Standards

The NIST "Security Risk Management Framework" (hereafter referred to as "Framework") has been developed by the Department of Commerce, and its use is mandatory for all federal agencies under the Federal Information Security Management Act (FISMA)[14]. It is devoid of conflict of interest and has been broadly and publicly vetted. There is nothing 'onerous' about the NIST Framework, as it applies specifically for systems that *do not* have national security significance, and recently it has been augmented to address the unique needs of industrial control systems. In a study performed by MITRE Corporation for NIST, a line-by-line comparison of controls and countermeasures within NIST SP800-53[15] and the NERC CIP Standards[16] was undertaken. The results indicated the NERC CIP Standards were less rigorous than even the low-baseline security controls established in the NIST Framework. In the final analysis, if U.S. Fish and Wildlife must comply with the low-baseline NIST Framework, from the perspective of societal wellbeing and economic stability, in good conscience is it prudent to require less from the operators of the electric grid.

A recurrent theme in the FERC NOPR is the need for greater granularity and detailed specificity in the CIP Standards. Part of the problem is the manner in which the CIP Standards are written – broadly brushed and highly generalized; so it's easy to understand FERC's desire for more specificity. This desire is at least in part motivated by the need to conduct compliance audits. The high-level abstraction of the NERC CIP Standards requirements language can leave the auditor struggling with shades of grey in interpretation (especially those auditors that come from a mainstream IT background exclusively), to say nothing as to grey-area impact in appeals to findings of non-compliance. In contrast, NIST SP800-53 is far more granular and provides clear requirements that have much less room for misunderstanding. Furthermore, the companion NIST SP800-53A[17] provides guidelines for determining the effectiveness of cyber security controls; that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security needs of the organization. Additionally, NIST has also produced a detailed guidance document for industrial control system (ICS) security, NIST SP800-82[18], which provides instruction on securing ICSs while at the same time satisfying their unique performance, reliability, and safety requirements.

---

[14] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, *et seq.*)

[15] National Institute of Standards and Technology Special Publication 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, December 2006.

[16] MITRE Technical Report (MTR070050): *Addressing Industrial Control Systems in NIST Special Publication 800-53*; http://csrc.nist.gov/groups/SMA/fisma/ics/documents/papers/ICS-in-SP800-53_final_21Mar07.pdf

[17] National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Third Public Draft), June 2007.

[18] National Institute of Standards and Technology Special Publication 800-82 (2nd draft), Guide to Industrial Control Systems (ICS) Security, http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

One of the major problems in control system cyber security is the culture clash between an organizations' mainstream IT department and that responsible for the operating critical infrastructure and related control systems. The NIST Framework, specifically NIST SP 800-53 extended for Industrial Control Systems (ICS), is the only document of which I am aware of that addresses both IT and control systems security in the same document. Consequently, it is my belief that this is a key tool that can help bridge the organizational divide between mainstream IT and control system operations functions; which in and of itself can help to untangle many of the existing control system cyber security issues.

Adoption of the NIST Framework for the electric sector will eliminate the requirement for redundant effort faced by a number of quasi-federal organizations such as the Tennessee Valley Authority (TVA) and the Bonneville Power Authority (BPA), who are now required to prepare different sets of documentation and endure dual audits for both FISMA and NERC CIP Standards compliance. Is this duplication a good use of ratepayer dollars?

The electric sector is arguably the most interdependent of all the critical infrastructures, and it's also the first of the private industrial sectors (health and financial excluded) to move toward establishment of cyber security standards. Without digression, it would appear wise for all of our industrial sectors to adopt a consistent set of methodologies for cyber security of distributed and process industrial control systems. The vulnerability demonstration shown by CNN (reference 5) provides a clear justification. The advisory notice about the demonstrated vulnerability was issued to the electric industry, including dams, and was also released to the chemical and water industries as they use similar systems and networks and thereby similar cyber vulnerabilities. Additionally, having consistent requirements across industries can minimize the potential for having to modify control systems to meet individual sector security requirements.

One way to move towards cross-sector convergence in cyber security ways and means is for all stakeholders to use the same terminology and to eliminate duplicative or overlapping sets of security standards' requirements. NIST offers a set of high-quality publications addressing most of the relevant managerial, administrative, operational, procedural, and technical considerations. Each of these publications, such as SP 800-53, have been put through a significant public vetting process by all sectors, including, to the extent possible, by authorities in the national security domain. NIST offers its documents to all organizations interested in using them as a basis for developing common Standards within the ICS community.

Summary Opinion

NERC is now FERC's Electric Reliability Organization (ERO) and as such should no longer be acting as an industry-representative organization. However, much evidence reveals NERC still exhibiting vestiges of its role as an industry advocate, at least in so far as concerns its attempts to minimize the urgency of the matter of cyber security. Rather than be attentive to and supportive of the FERC NOPR and move to assure its implementation, NERC has chosen to issue rebuttal comments[19]. What's more, the dubious act of NERC submitting a rebuttal to FERC is exacerbated by the poor technical quality of its comments. NERC has not had previous experience with control system cyber security, and I do not believe that NERC as constituted is capable of providing adequate oversight of cyber security of the grid.

For the reasons stated above, the existing NERC CIP Standards are not adequate for cyber-securing the electric grid. There are other approaches that can provide a higher level of security without incurring significant incremental cost. My principal recommendation is that the NIST Framework's requirements

[19] NERC Comments on the FERC NOPR dated October 5, 2007, Comments on the North American Electric Reliability Corporation on the Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection, nerc.com

should be incorporated into standards for industry that are currently being developed by the ISA99 Standards Development Committee, Security for Industrial Automation and Control Systems[20]. As is NERC, ISA is an accredited member organization of the American National Standards Institute, and the ISA99 committee brings together security experts from across industry, government, and academia. DHS has already provided valuable support by allowing experts from NIST and the National Laboratories to contribute in this ISA99 initiative, and it is vital that this support continue. I recommend further that the NIST Framework requirements form the basis of compliance audits to be conducted by a new and related entity, the ISA Security Compliance Institute. Any resulting fines or other findings should be addressed by NERC. A single set of Standards for industrial automation and control systems is more cost effective than a patchwork of standards conceived independently by each industrial sector. This would provide the leading practitioners on control systems cyber security to bring their expertise to bear and provide comparable levels of protection across the interdependent critical infrastructures.

Recommendation to Congress

Congress should empower FERC with the authority and responsibility for development of control system cyber security requirements and compliance criteria similar to role of NRC in these matters. In so doing, Congress should also provide FERC with the authority to separate ERO functions so that NERC is responsible for traditional electric system reliability Standards, and have a separate organization be responsible for the cyber security aspects of critical infrastructure protection. Finally, Congress should take action so that the ERO function is funded by the government, not by industry as is now the case, to better ensure that conflicts of interest do not interfere with doing what is right and necessary, and not just what is convenient.

Thank you for your interest,
Joseph Weiss, PE, CISM
Applied Control Solutions, LLC

[20] ISA99, Security for Industrial Automation and Control Systems